Homeland Security

NIPP-Cyber Security

National Infrastucture Protection Plan

DHS Cyber Security

Critical infrastructure and Key Resources (CI/KR) support the essential functions and services that underpin American society. Some CI/KR elements are so vital that their destruction, incapacitation, or exploitation through a terrorist or type of other attack, could have a debilitating impact on national security and economic well-being. Homeland Security Presidential Directive-7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," issued in December 2003, directs Homeland Security to produce a comprehensive, integrated national plan for CI/KR protection. HSPD-7 also designates Homeland Security as a national focal point for the security of cyberspace.

The NIPP Helps Protect Our Critical Infrastructure

In response to HSPD-7, Homeland Security and its government and private sector partners are developing and implementing the National Infrastructure Protection Plan (NIPP). The draft NIPP Base Plan was issued for public comment in November 2005. The final NIPP Base Plan is expected to be released in early 2006. The NIPP provides a consistent, unifying structure for integrating current and future CI/KR protection efforts. The Department's cyber security division is responsible for the cyber elements of the NIPP as part of implementing a cyber risk management program to enhance security and mitigate the risk of attack across all CI/KR. The cyber elements of the NIPP include the Information Technology (IT) sector and the cross sector cyber risk.

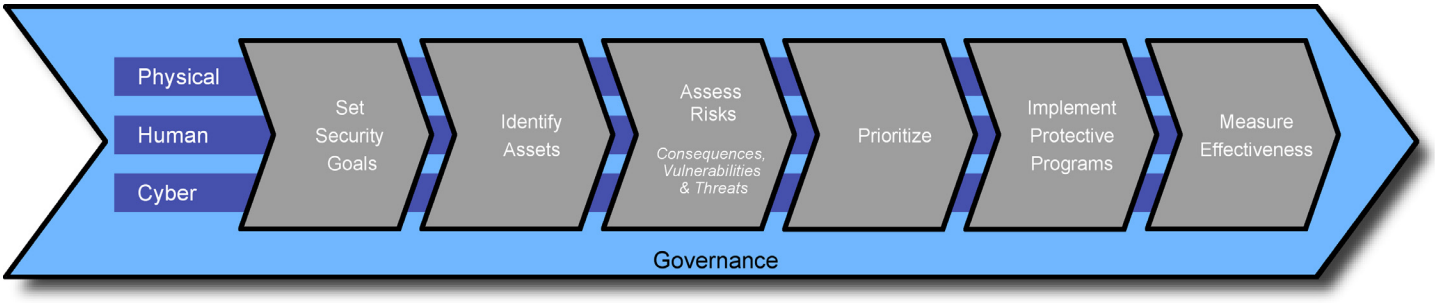
Implementing the Cyber Elements of the NIPP

The U.S. economy and national security are highly dependent upon the cyber infrastructure. Cyber infrastructure enables the Nation's essential services, resulting in a highly interconnected and interdependent network of CI/KR. The term "cyber" refers to electronic information and communications systems and the information contained therein. Information and communication systems are comprised of all the hardware and/or software that processes, stores, and communicates information. To reflect the increasing convergence of IT and telecommunications in our communication networks, the Department's cyber security division works closely with the National Communications System (NCS) to address related issues. One clear example of such collaboration involves the cyber security division and the NCS leading an effort to address Internet disruption concerns.

CI/KR sectors' functions and services are enabled through cyber systems and services. The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's risk to cyber threats if cyber security is not addressed and integrated appropriately. To address this cyber risk, the NIPP includes a cross-sector cyber element, as well as an IT Sector responsibility.

National Risk Management Framework

Providing a framework to achieve the goals outlined in the NIPP



Engaging with the IT Sector

The IT Sector produces hardware, software, and services that enable other sectors to function. The Department's cyber security division is the Sector Specific Agency (SSA) for the IT Sector and leads the IT Sector Government Coordinating Council (GCC). The Department's cyber security division and the IT GCC are collaborating with the IT Sector Coordinating Council (SCC) to identify, prioritize, and coordinate the protection of IT CI/KR. In addition, Homeland Security encourages continued cooperation through the IT SCC to facilitate sharing of information about threats, vulnerabilities, incidents, protective measures, and best practices.

Addressing Cross-Sector Cyber Risk

The cross-sector cyber responsibility is a collaborative effort between the Department's cyber security division and SSAs to improve the cyber security of the critical infrastructure sectors by facilitating cyber risk reduction activities. The Department's cyber security division provides cyber guidance to all sectors to assist them in understanding and mitigating cyber risk (including cyber infrastructure vulnerabilities) and in developing effective and appropriate protective measures.

In addition to SSAs' efforts, cyber security is a concern to individuals because of their increasing reliance on the cyber infrastructure, including the Internet. Individuals play a significant role in managing the security of their computer systems and preventing attacks against CI/KR. Therefore, Homeland Security's cyber security public awareness efforts are key to reducing overall cyber risk.

Building Success through Relationships

For the NIPP to be successful, there must be integrated and effective public-private partnerships, as well as communication and coordination at all levels. Therefore, Homeland Security and SSAs are discussing the NIPP with security partners to collaboratively identify and support the planning and information mechanisms that make the most sense and will be most effective for CI/KR protection.

The NIPP encourages the following two partnerships to enable government and private sector partners to undertake the full range of protective activities:

- **Sector Coordinating Councils** – Provides a framework for private sector infrastructure owners and operators and supporting associations to engage with Homeland Security and SSAs.
- **Government Coordinating Councils** – Provides a forum for interagency communication, coordination and partnership with Homeland Security, SSAs, and the supporting Federal departments and agencies that have a role in protecting the respective sectors.

Working Together to Secure Cyberspace

Homeland Security is committed to securing cyberspace by working collaboratively with public, private, academic, and international entities to ensure that CI/KR owners and operators are adequately prepared to foresee and, if possible, reduce the likelihood of cyber attacks; and that the CI/KR cyber elements are able to:

- Withstand attacks without incurring catastrophic damage;
- Respond and recover from attacks in a timely manner; and,
- Sustain nationally critical operations.

Obtaining Additional Information

To learn more about the cyber element of the NIPP, contact the NIPP Program Management Office at: NIPP@dhs.gov

Cyber security is a shared responsibility. Working together, we can secure America's cyberspace.